

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF:
13413 YORKTOWN DRIVE,
BOWIE, MARYLAND

Case No. GLS-19-1100

Filed Under Seal

FILED
LODGED

ENTERED
RECEIVED

AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE

MAY 31 2019

AT GREENBELT
CLERK U.S. DISTRICT COURT
DISTRICT OF MARYLAND

I, Daniel E. Beresh, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as **13413 Yorktown Drive, Bowie, Maryland**, hereinafter “**PREMISES**,” further described in Attachment A, for the things described in Attachment B.
2. I am a Special Agent with United States Immigration and Customs Enforcement (“ICE”), Homeland Security Investigations (“HSI”), and have been so employed since April 2003. I am presently assigned to the Office of the Special Agent in Charge, Baltimore, Maryland, where I am responsible for conducting criminal investigations involving the illegal importation and exportation of goods and services from the United States. Prior to my appointment with HSI, I was employed as a sworn peace officer in the State of Maryland for approximately seven years.

3. I have been the primary, secondary, and/or tertiary agent on numerous investigations which involved transnational criminal endeavors to include those associated with

cyber and narcotics investigations. During these investigations, I have conducted searches, seizures, and arrests. I have conducted multiple interviews with members of transnational criminal organizations and developed information and expertise using various investigative techniques. Additionally, I have received training in the methods, devices, and customs common to individuals and organizations involved in international crime. Through this training and experience, I have become familiar with the methods and techniques used by individuals to promote and facilitate unlawful activity. This training and experience forms the basis for the information expressed below. The following is based on oral and written reports by me and other law enforcement agents, surveillance, subpoenaed and public records, database checks, phone analysis, and other such investigative findings.

4. The information in this affidavit includes facts known personally to me, as well as facts that I have learned from other agents involved in the investigation, as well as review of reports and other documents. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

APPLICABLE LAW OF CRIMES UNDER INVESTIGATION

5. I submit this affidavit in support of an investigation into crimes including, but not limited to, violations of the following statutes.

6. **Wire Fraud (18 U.S.C. § 1343):** "Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings,

signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.”

7. **Attempt and Conspiracy (18 U.S.C. § 1349):** “Any person who attempts or conspires to commit any offense under this chapter [including 18 U.S.C. 1343] shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.”

8. **Aggravated Identity Theft (18 U.S.C. § 1028A(a)(1)):** “Whoever, during and in relation to any felony violation enumerated in subsection (c) [including 18 U.S.C. 1343], knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.”

PROBABLE CAUSE

Background

9. In March of 2018, Homeland Security Investigations (“HSI”) Detroit initiated an investigation into a group of individuals who referred to themselves as “The Community.” The Community was a loosely organized group of individuals dedicated to online identity theft. Its members specialized in a tactic known as “SIM Hijacking” or “SIM Swapping.”

10. This tactic enabled The Community to gain control of a victim’s mobile phone number by linking that number to a subscriber identity module (“SIM”) card controlled by The

Community—resulting in the victim’s phone calls and short message service (“SMS”) messages being routed to a device controlled by a member of The Community.¹

11. Upon gaining control of a victim’s mobile number, one or more members of The Community would proceed to access an online account of the targeted victim by either (1) cracking (or stealing) a password and then requesting a two-factor authentication (“2FA”) code be sent to the impersonating device or (2) requesting that a password be reset via a text message. Once an initial account—typically an email account—was compromised, The Community would next seize control of additional accounts by resetting additional passwords linked to the initial account that they now controlled.

12. During these attacks, one or more members of The Community would appropriate the online identity of the victim, using means of identification including the victim’s name, email, and mobile phone number.

13. Members of The Community planned and organized their activities on various online forums and over diverse channels of communication. Broader discussions—such as discussing the manner and means of attacks generally, and networking among The Community’s members—typically took place on forums such as “OGUsers” and “Hackforums.”² Planning and

¹ In this investigation, SIM Hijacking was often facilitated by bribing an employee of a mobile phone provider. Other times, SIM Hijacking was facilitated by “social engineering”: e.g., a member of The Community would contact a mobile phone provider’s customer service—posing as the victim—and request that the victim’s phone number be swapped to a SIM card (and thus a mobile device) controlled by The Community.

² These forums are typically publically accessible, but require registration and moderator approval to join.

execution of specific attacks, as well as victim selection and recruiting, usually took place via encrypted or real-time platforms such as Discord, Skype, Signal, Wickr, and Telegram. These services can be accessed by the use of computers, as well as by mobile devices such as phones and tablets.

14. The investigation revealed that a subset of The Community conspired to specialize in the theft of cryptocurrency.³ These individuals engaged in SIM Hijacking with the goal of gaining control of—and stealing—a target’s cryptocurrency.

15. The conspirators would conduct research to identify targets for SIM Hijacking that were publicly associated with cryptocurrency, such as investors or promoters. The assumption of the conspirators was that these individuals would have substantial cryptocurrency holdings.

16. If the conspirators were able to successfully hijack a target’s phone number, they would use the techniques above to attempt to steal the target’s cryptocurrency.

17. In May of 2018, a member of The Community (CM1) was arrested and began cooperating with law enforcement. On or about May 23, 2018, law enforcement gained access to records of online chats between members of The Community via forensic extractions of the CM1’s devices, as well as the devices themselves. Law enforcement further conducted in-person interviews of CM1 on June 7, 2018; June 28, 2018; and August 1, 2018. In these interviews,

³ Cryptocurrencies, also known as virtual currencies or digital currencies, are online media of exchange. The most famous is Bitcoin, but many others exist—such as LiteCoin and Ethereum. Like traditional currency, cryptocurrencies act as a store of value and can be exchanged for goods and services. They can also be exchanged for dollars. But, unlike “fiat” currencies such as the dollar, they are untethered from the traditional banking system and are neither issued nor backed by sovereign states. Their value depends only on the law of supply and demand.

CM1 identified members of The Community, their roles, and their usernames, including via Skype.

18. On June 25, 2018, a state search warrant was issued to Microsoft (Skype) by the 35th District Court of Wayne County, Michigan for Skype user accounts, which enabled the further review of online chats between members of The Community.

19. On or about July 16, 2018, law enforcement received the search warrant response from Microsoft for the Skype user accounts. This return included chat messages involving members of The Community, account registration reports, and IP addresses linked to accounts.

20. Between May 2018 and August 2018, an HSI Detroit analyst with knowledge of the investigation conducted reviews of CM1's devices, the forensic extractions of those devices, and chat logs obtained from search warrant responses. This review identified over 100 conversations between members of The Community discussing the planning and execution of cryptocurrency thefts from various victims that had occurred from at least January 2018 to June 2018. Subsequent search warrants were issued for chat logs for additional usernames of members of The Community that were engaged in SIM swapping and stealing cryptocurrency.

21. In most conversations that targeted a victim for cryptocurrency, a member of The Community would provide personally identifiable information (PII) of the victim, which would typically include the victim's name, phone number, and known email addresses. Members of The Community would then provide a new SIM card number to activate for the victim's phone number and/or the IMEI (International Mobile Equipment Identity) of the device held by a member of The Community. An IMEI is the unique identifier assigned to each mobile telephone – that is, the physical handset (e.g., Apple, Samsung, Android phone) – to which a particular call

number is assigned. Members of The Community would also provide cryptocurrency addresses in the chats in which to receive their cut of any cryptocurrency theft.

22. In early August 2018, an HSI Detroit analyst wrote Visual Basic for Applications (VBA) scripts that enhanced the identification of potential victim email addresses, potential victim phone numbers, suspect cryptocurrency addresses, suspect SIM card numbers, and suspect IMEIs. An HSI Detroit analyst subsequently generated lists of potential victim and suspect data based on chat logs covering between approximately November 2017 and July 2018.

23. In August 2018, an HSI Detroit analyst contacted investigators at U.S.-based phone carriers regarding potential SIM swapping activity with victim phone numbers, as well as suspect SIM cards and suspect IMEIs. Based on information received from two phone carriers and further review of chat messages, over 200 victims of SIM swapping by members of The Community were identified between November 2017 and July 2018, including victim SB, as further detailed below.

24. Between May 2018 and October 2018, law enforcement personnel conducted or attempted phone interviews of over 50 of the suspected SIM swapping victims in order to verify the SIM swap, determine if any accounts were hacked, and substantiate any cryptocurrency losses. The interview of Victim SB, the focus of this affidavit, occurred on October 1, 2018.

25. In November 2018, law enforcement obtained additional information on victims with cryptocurrency thefts or attempted thefts from their mobile phone providers and online service providers. This information revealed unauthorized access to the victims' phone services as well as email, cloud storage, and cryptocurrency exchange accounts. In numerous instances,

law enforcement was able to identify an IP address or addresses⁴ that one or more attackers used to access a victim's online accounts.

26. In March 2019, law enforcement conducted a search warrant at the residence of a known member of The Community. During a voluntary interview, the member provided consent for law enforcement to take over his online accounts, including Wickr, Discord, and Skype accounts. An HSI Detroit analyst reviewed the Skype account, which identified that members of The Community continued to engage in SIM swapping and attempted cryptocurrency theft through at least February 2019.

27. In total, based on the victims identified, including SB, this investigation has obtained evidence that between approximately February 15, 2018 and May 19, 2018, members of The Community have been responsible for thefts of cryptocurrencies in excess of \$2,400,000 (as valued at time of theft). The thefts were all coordinated and executed via the Internet utilizing several internet platforms, to include Discord⁵ and Skype, with the intent to hide or disguise the members' true identities. Proceeds from the cryptocurrency thefts were disbursed electronically and in anonymity due to the nature of cryptocurrency transactions.

⁴ The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

⁵ Discord is a proprietary freeware voice over internet protocol application specializing in text, image, video and audio communication between users in a chat channel.

Individual 1⁶

28. Through a review of online chats, information provided by CM1, and the results of the Skype search warrant, Skype user drinkingmilk8 was identified as a member of The Community who engaged in SIM swapping and cryptocurrency theft. Specifically, on or about July 16, 2018, an HSI Detroit Task Force Officer received a search warrant response from Microsoft that included Skype user drinkingmilk8. Microsoft's response included chat history from January 13, 2018 to June 25, 2018, IP addresses, a registration report, and an account report for user, drinkingmilk8.

29. This information established that, on or about May 13, 2018, the user drinkingmilk8 provided the personal identifying information of at least five potential victims, including Victim SB described further below.

30. The Skype chats further indicate that user drinkingmilk8 also participated in at least 22 conversations from January 13, 2018 to June 25, 2018 in furtherance of SIM swapping activity. These conversations contained an estimated 77 phone numbers suspected to belong to potential victims.

31. During the course of the investigation, through IP address information, Skype registration information, and physical surveillance, investigators obtained evidence establishing probable cause to believe that Skype user drinkingmilk8 is Individual 1 of Bowie, Maryland.

⁶ At the time of the offense described herein, Individual 1 was a juvenile. Although Individual 1 is now an adult, to protect Individual 1's identity, it is not disclosed. Individual 1's true identity is known to me and other law enforcement agents involved in this investigation.

32. From the Microsoft search warrant response, an HSI Detroit analyst compiled the available IP addresses and date ranges for drinkingmilk8, which included the following IP addresses belonging to the internet service provider Verizon in the vicinity of Bowie, Maryland:

| IP Address | Count | Start (UTC) | End (UTC) |
|---------------------|----------|----------------------------|----------------------------|
| 96.231.149.98 | 11 | 12/31/2017 03:40:15 | 01/30/2018 00:54:43 |
| 71.120.6.250 | 9 | 04/26/2018 23:57:13 | 05/15/2018 23:26:15 |
| 96.255.193.247 | 8 | 08/30/2017 19:18:57 | 11/05/2017 19:04:16 |
| 96.231.38.73 | 6 | 05/19/2018 18:51:48 | 05/25/2018 23:14:07 |

33. Further analysis of the search warrant return from Microsoft revealed that between April 26, 2018 and May 15, 2018, Individual 1 was utilizing IP address 71.120.6.250 while he was chatting with others to facilitate the attacks on at least one victim of The Community—to wit, Victim SB further discussed below.

34. An HSI Detroit analyst reviewed the Skype account report which identified Skype user drinkingmilk8 as an alias of an account with an email address of rXXXX@gmail.com. As of July 10, 2018, the display name for that Skype account was Individual 1's true name.

35. On July 31, 2018, an HSI Detroit Task Force Officer received a response from Verizon for IP addresses 96.231.149.98, 71.120.6.250, 96.255.193.247, and 96.231.38.73. Subscriber records for all four IP addresses returned to 13413 Yorktown Drive, Bowie, Maryland, i.e., the PREMISES. Using law enforcement and commercial databases, an HSI Detroit analyst identified Individual 1 as residing at the PREMISES.

36. In October 2018, HSI Detroit personnel conducted a telephonic interview of CM1. CM1 verified that Individual 1 was a SIM swapper that he had worked with prior to his arrest in May 2018.

37. On or about November 20, 2018, members of the Regional Enforcement Allied Computer Team (REACT) Task Force in Santa Clara County, California received information from a cooperating individual (CM2) who was a member of The Community. CM2 stated that Individual 1 lives in Bowie, Maryland. CM2 stated that Individual 1 has been involved in around \$1.5 million worth of SIM swaps and has worked with six others; the six individuals provided by CM2 are known by HSI Detroit to be members of The Community. CM2 stated that Individual 1 recently found a way to get into a T-Mobile tool; CM2 stated that Individual 1 was the only person in the world that could do T-Mobile phones with tools who isn't an employee. CM2 stated that Individual 1 has gambled most of what he has made and has spent a good amount of it on clothes. CM2 stated that Individual 1 was not very well known in The Community, but he has done a lot of swaps. CM2 stated that Individual 1 was involved in a \$1 million attack with "N.T.," an identified member of The Community. CM2 stated that Individual 1 was given \$40,000 for putting Google Authenticator on the victim's email.

38. There is also evidence that Individual 1 continued to engage in SIM swapping activities through at least February 2019. In April of 2019, an HSI Detroit analyst reviewed chat messages for a Skype account that law enforcement had taken over from a known member of The Community. This Community member consented to the takeover of his accounts in March of 2019. Review of the cooperating member's chat messages resulted in the identification of six conversations with Skype user account, "live:dsfgsgfdgvrefgegr3" between January 12, 2019 and

February 28, 2019; each of these conversations involved SIM swapping and attempted cryptocurrency theft, with one conversation containing approximately 32 phone numbers of potential victims. In two of the conversations, with two different members of The Community, the user of “live:dsfgsgfdgvrefgegr3” is addressed by Individual 1’s true first name.

39. On May 7, 2019, an HSI Detroit analyst reviewed information from a financial institution used by Individual 1. This review identified an incoming wire credited to Individual 1 on November 19, 2018 in the amount of \$30,519.54 from originator Gemini Trust Company LLC. Gemini Trust Company LLC is a U.S.-based cryptocurrency exchange.

Victim SB

40. Victim SB is one particular victim of The Community whom Individual 1 helped attack. On August 14, 2018, an AT&T investigator provided information on IMEIs suspected to be involved in SIM swapping to an HSI Detroit analyst. The records from AT&T showed that on May 13, 2018, a new SIM card was activated for phone number XXX-XXX-9611 (SB’s mobile phone number) on IMEI 359230063339584. Based on search warrant returns from AT&T, on May 13, 2018, this IMEI was located in vicinity of Eagle, Idaho. A known member of The Community lives in this area, while SB does not.

41. As described above, on or about May 13, 2018, Individual 1, as Skype user drinkingmilk8, participated in a Skype chat furthering a scheme to defraud victim SB of his cryptocurrency. Individual 1 and others conspired to use SB’s identity to seize control of multiple online accounts—including an email account and a cryptocurrency exchange account.⁷

⁷ Also, on May 13, 2018, Individual 1 provided the personal identifying information of at least 4 other potential victims, as further discussed below in the section entitled “Other Victims.”

42. Individual 1 provided SB's email addresses and phone number, which were used to facilitate this attack. Within twenty minutes of Individual 1's posting of SB's information, SB's phone number was swapped to a new device. Another known member of The Community then proceeded to compromise SB's accounts, including SB's cryptocurrency account; this member posted passwords in the group conversation, as well as pasted historical cryptocurrency transaction information from a Citibank account for SB.

43. On October 1, 2018, SB informed an HSI Detroit analyst that his phone number was hacked on Mother's Day 2018. SB stated that he had a Coinbase account,⁸ but he was not actively trading. SB stated that his Citibank account was linked to his Coinbase account. SB stated on the day of the phone hack, the hackers attempted to wire approximately \$15,000 from his Citibank account to Coinbase.

44. On or about November 13, 2018, Coinbase provided a subpoena response regarding SB's account. This response revealed that on May 13, 2018, there were login events from a new device. Within ten minutes of this new login, there was an "email sent" event, which stated that "Your purchase for \$15,000.00 USD of BTC has started."

Victim RR

45. Victim RR is a second victim from whom there is evidence that Individual 1 helped steal cryptocurrency. According to the REACT Task Force, on or about October 26, 2018, victim RR lost approximately \$1,000,000 in U.S. dollars from two cryptocurrency

⁸ Coinbase is a cryptocurrency exchanger through which users may purchase various cryptocurrencies in exchange for fiat currency, such as U.S. dollars.

exchanges as a result of a SIM swap. After the SIM swap, the suspects purchased Bitcoin with the U.S. dollars on the exchange account and transferred the Bitcoins out.

46. On November 14, 2018, the REACT Task Force arrested Community Member NT for his participation in the SIM swap and theft of victim RR. According to REACT, NT admitted to working with Individual 1, but did not mention any specific attacks.

47. As mentioned previously, on or about November 20, 2018, CM2 stated that Individual 1 was involved in a \$1 million attack with NT, an identified member of The Community. CM2 stated that Individual 1 was given \$40,000 for putting Google Authenticator on the victim's email.

48. In January of 2019, the REACT Task Force received a statement from a cooperating individual (CM3) who was identified as a suspect in the theft of RR. CM3 admitted to participating in the theft of RR and named Individual 1 as participating in the hack. CM3 further stated that Individual 1 received approximately \$50,000 in cryptocurrency as a result of the theft.

Other Victims

49. In May of 2019, an HSI Detroit analyst reviewed the entire group conversation containing the hack of SB that involved Individual 1 and other known members of The Community. This review identified two group voice calls lasting a total of approximately 4 hours and 32 minutes between May 13, 2018 at 20:30:28 UTC and May 14, 2018 at 01:04:11 UTC. Further review of the group conversation identified that Individual 1 provided additional victim information on May 13, 2018 as detailed below.

50. Starting at 20:31:10 UTC, Individual 1 provided email addresses for victim MD. Another member of The Community provided MD's phone number, XXX-XXX-0150, at 20:34:24 UTC. The records from AT&T show that new SIM cards were activated for XXX-XXX-0150 at approximately 20:30:55 UTC on IMEI 359230063339584 and at approximately 20:53:21 UTC on IMEI 359306063090979. Both IMEIs were located in the Southern Idaho market, where a known member of the Community lives.

51. Starting at 20:45:59 UTC, Individual 1 provided name, phone number XXX-XXX-9023, and email addresses for victim RS. The records from AT&T show that a new SIM card was activated for XXX-XXX-9023 at approximately 21:43:22 UTC on IMEI 359306063090979.

52. At 22:01:14 UTC, Individual 1 provided name, email addresses, and phone number XXX-XXX-7745 for victim AL. The records from AT&T show that a new SIM card was previously activated for XXX-XXX-7745 on May 9, 2018 on IMEI 359306063090979. HSI Detroit identified that victim AL lost 6 Bitcoin from his cryptocurrency account over three days in relation to the May 9, 2018 SIM swap.

53. Starting at 22:03:03 UTC, Individual 1 provided the name, email address, and phone number XXX-XXX-2727 for potential victim CG. An unauthorized SIM swap of this phone number could not be verified.

54. Starting at 23:06:24 UTC, Individual 1 provided an email address and phone number XXX-XXX-4664 for victim JD. The records from AT&T show that a new SIM card was activated for XXX-XXX-4664 at approximately 23:30:24 UTC on IMEI 359230063339584.

Individual 1 further provided images via printscr.com that included JD's social security card, a vehicle registration for JD, and images of JD with his driver's license.

55. On or about September 6, 2018, victim JD provided information to HSI Detroit personnel that included a screenshot showing that victim JD's Facebook account was accessed from IP address 71.120.6.250 (the same address used by Skype user drinkingmilk8, registered to the PREMISES, as described above) and a screenshot showing that his Apple ID was signed in near Bowie, Maryland. Victim JD informed HSI Detroit personnel that the hacker threatened to shut down his business domain if he did not "hand over the Bitcoins." JD informed HSI Detroit personnel that the hacker took his business services offline for up to 72 hours because he did not provide Bitcoin.

13413 Yorktown Drive, Bowie, Maryland, i.e., the PREMISES

56. According to an April 21, 2019 inspection of Individual 1 by U.S. Customs and Border Protection, when Individual 1 entered the United States, Individual 1 stated he resides with his parents at the PREMISES.

57. On April 24, 2019, a United States Postal Inspection Service Inspector informed HSI Detroit that on April 22, 2019, Individual 1 received mail at 13413 Yorktown Drive, Bowie, Maryland, i.e., the PREMISES. Individual 1 also received mail at this address on April 23, 2019.

58. On April 30, 2019 at approximately 7:20 a.m., an HSI Baltimore Special Agent established physical surveillance of the PREMISES. The residence is a single-family, two-story home made of gray brick and gray siding. It has a dark colored front door. The numbers

“13413” appear in black writing on a white backdrop attached to the façade of the home.

Additionally, a sign bearing the numbers “13413” is planted in the front yard of the residence.

59. On this same date, the HSI agent witnessed Individual 1 leave from the front door of the PREMISES and briefly approach a 2015 Tesla Model S bearing Maryland registration 7DP6564 parked in the driveway. Individual 1 then returned to the house through the same entry. A search of Maryland Motor Vehicle Administration records found the 2015 Tesla was registered to Individual 1 at the Yorktown Drive address, i.e., the PREMISES.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

60. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

61. As set forth in this affidavit, Individual 1 is suspected of participating in a conspiracy that was primarily active between January of 2018 and at least February of 2019. Evidence of these crimes is likely to be found at his residence for, including but not limited to, the following reasons:

- a. An electronic device such as a computer, tablet, or smart phone (or some combination of these devices) was used to commit these crimes. As described in more detail below, electronic evidence is persistent. In many cases evidence of a crime can be recovered from an electronic device even if it was deliberately

deleted by the user. I also know, from my training and experience, that computers and other electronic devices are replaced infrequently, and that many people save and store computers that are no longer in use to protect their personal data.

- b. The investigation has gathered evidence that Individual 1 participated in the planning and execution of SIM swapping and cryptocurrency theft using unique online identities. I know, from my training and experience, that—in order to maintain continuity of online relationships—people commonly continue to use the same online identities (or variations of these identities) for years, even across different communications platforms. Evidence of the continued use of identities involved in SIM swapping and cryptocurrency would link Individual 1 to his previous crimes, even if his involvement in these activities has ceased.
- c. The goal of the conspiracy in which Individual 1 was involved was the theft of cryptocurrency. As described elsewhere in this affidavit, cryptocurrency is a virtual asset that is stored and transferred using electronic devices, software wallets, or third party services. Without continued access to their personal passwords, recovery seeds, hardware wallets, software wallets, and/or exchange accounts, an individual would lose access to their cryptocurrency. Therefore it is highly unlikely that the unique tools that a cryptocurrency user needs to access their assets would be abandoned. This holds true regardless of in what form an individual stores their cryptocurrency. In addition, even if Individual 1 transferred cryptocurrency stolen from his victims into other assets, records involving those transactions could likely be recovered from his electronic devices

62. Accordingly, I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer

users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

63. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the

sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion.
- i. In my training and experience, information stored within a computer or storage media (e.g., registry information, personal communications, personal images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- ii. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner.
- iii. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity

associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.

iv. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user.

v. Information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password

protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to obtain unauthorized access to a victim's online accounts over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a

storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

64. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic

electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

65. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted

scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

66. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

SEARCHES FOR EVIDENCE PERTAINING TO CRYPTOCURRENCY

67. As described *supra*, this investigation involves the theft of cryptocurrency.

68. Cryptocurrency is stored in “wallets” both online and offline. In order to access and send the cryptocurrency stored in these wallets, the owner of the cryptocurrency must have access to both the wallet address, also known as a public key, and the private key. Both the wallet address and private key are lengthy, facially unintelligible, strings of letters and/or numbers.

69. Recovery seeds are a series of random words which store the information needed to recover all of the public key-private key pairs of a cryptocurrency wallet. Recovery seeds allow an owner of virtual currency to access his/her wallet from any electronic device.

70. Cryptocurrency can be—but is not necessarily—stored in so-called “hardware wallets,” physical devices produced by companies such as SatoshiLabs or Ledger that contain the wallet addresses and private keys necessary to access and transfer cryptocurrency. A user of such

a device may store the password or passwords necessary to access such an account on a phone, computer, or other electronic storage device.

71. Cryptocurrency can be—but is not necessarily—stored in online wallets, some of which are controlled by the operators of online cryptocurrency exchanges. In the case of a user of an online wallet, electronic devices such as phones or computers would contain records pertaining to its access. A user may also store the password or passwords necessary to access such an account on a phone, computer, or other electronic storage device.

72. Some cryptocurrency owners write their private keys, wallet addresses, recovery seeds and/or passwords down or print them out on paper and hide them in various places such as picture frames, safes, desks, etc., as backup so that they do not lose access to their wallets.

73. Some cryptocurrency owners store their private keys, wallet addresses, recovery seeds, and/or passwords on their computers, cell phones, or other electronic storage devices. On an electronic storage device, such keys, addresses and passwords can be stored in any form and—like other valuable electronic information—are sometimes concealed or encrypted. Concealment of electronic files can take place by many means, including but not limited to renaming files, changing file extensions, hiding files in unusual places (such as among word

processing documents or photographs), or using various publically available programs to encrypt or hide them.

74. Some cryptocurrency owners will take pictures of their private keys, wallet addresses, recovery seeds, and/or passwords and store them electronically. Such photographs may be concealed or encrypted as described in the preceding paragraph.

75. In my training and experience, cryptocurrency users closely control access to cryptocurrency. The information used to access and transfer cryptocurrency—as well as the electronic devices used to do so—will typically be located on the person of a cryptocurrency user, at their home, and/or at another secure location readily accessible to the user.

76. In my training and experience, users of cryptocurrencies—especially those that have stolen it—often convert one cryptocurrency into another. For those that have stolen cryptocurrency, these transfers are often done to attempt to conceal stolen funds and make them more difficult to trace.

77. There is a myriad of cryptocurrencies, including but not limited to Bitcoin, Ethereum, Ripple (XRP), Bitcoin Cash, Litecoin, EOS, Binance Coin, Stellar, Cardano, Monero, Zcash, Dash, Dogecoin, and Verge.

CONCLUSION

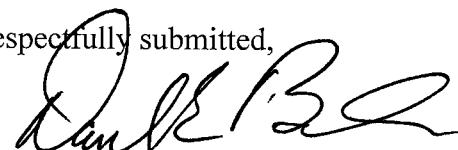
78. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

79. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application

and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,



Daniel E. Beresh
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me
On May 8, 2019



HON. GINA L. SIMMS
UNITED STATES MAGISTRATE JUDGE